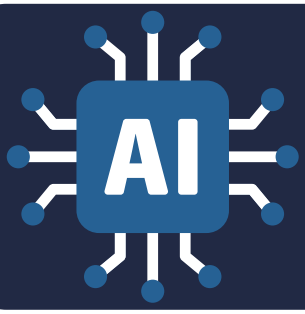
AI READINESS CHECKLIST

Preparing Your Organization to Add AI Tools to Your Anti-Fraud Program



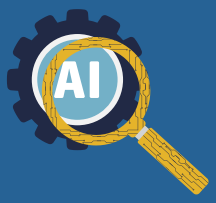
According to the 2026 *Anti-Fraud Technology Benchmarking Report*, **25%** of organizations stated that they use artificial intelligence (AI)/machine learning in their anti-fraud data analysis initiatives, with an additional **28%** expecting to adopt it over the following two years.*





Adoption is also expanding beyond analysis. As part of the 2026 report, **59%** of organizations "currently use or expect to deploy" generative AI/large language models (LLMs) within the next one to two years, while **64%** "currently use or expect to deploy" agentic AI.*





Within the fraud threat landscape, only **7%** of anti-fraud professionals believed their organization was more than moderately prepared to detect or prevent AI-powered fraud.*





AI adoption should come with careful consideration of potential impacts and risks. Before introducing a new AI tool to your team or organization, consider what you expect it to do, what information it will use, and what could happen if its results are inaccurate or incomplete.

Use this exercise to guide that conversation.
Choose an AI tool or use case that your organization is considering. On your own or with your team, discuss the questions below, then use the space provided to capture your response.

**Data from the 2026* Anti-Fraud Technology Benchmarking Report*, created by the Association of Certified Fraud Examiners (ACFE) in partnership with SAS.*

1 Define the Purpose

Before selecting or implementing an AI tool, clarify what you want it to accomplish and how you will know whether it is providing value.

- Why would this tool be important to our work?
- What specific parts of our processes could AI improve?
- What would a useful result look like in practice?
- How will we measure whether the tool is improving the use case?

Based on our answers, we want to use AI to:

2 Consider Your Data and Requirements

Next, understand what information the AI tool will access and what requirements apply to its use.

- What data will the AI tool access?
- Is our data readable and in the appropriate format?
- Would the tool use confidential, personal or sensitive information?
- How is information entered into the tool stored, used and protected?
- What regulations or internal policies apply to AI and data access?
- Does using the tool require approval, documentation or compliance review by IT, legal or another designated function?

One requirement or question we need to resolve:

3 Plan for AI Results

Think through how AI results will fit into your existing process and what safeguards are needed before acting on them.

- Which tool or platform best fits our needs?
- Before using a tool, what should we evaluate about the provider and intended use?
- Who will be responsible for independently verifying the tool's results?
- What happens next if a result is incomplete, inconsistent or unexpected?
- What are the potential consequences of an incorrect result?

How will human review be included alongside the tool we select?

4 Test Outcomes and Effectiveness

Put the AI tool through realistic scenarios to test how it performs in practice, not just how it is expected to perform.

- Check accuracy and consistency of results against known conclusions.
- Trial with multiple stakeholders and gather feedback.
- Document unexpected or inconsistent results.

Where does this AI tool have limitations, or do we need more time to understand how it will fit our needs?

5 Plan for Implementation and Ongoing Review

If the tool moves forward, consider what will be needed to implement it responsibly and maintain appropriate safeguards over time.

- Determine who should have access and what permissions they need.
- Prepare employees to use and interpret results.
- Document policies and expectations for use.
- Establish how performance and accuracy will be monitored.
- Revisit the tool as its capabilities, data, risks or organizational needs change?

Before we rely on this tool, we need to:

Keep the Conversation Going

AI can help organizations strengthen anti-fraud efforts, but responsible adoption starts with understanding the risks, requirements and safeguards involved. Before introducing a new tool, consider how it fits within your organization's policies, security practices, existing processes and customer needs.



If this exercise surfaced questions, bring them to your team and stakeholders for discussion. Taking the time to consider how AI fits into your processes, where its limitations may lie and where human judgment remains essential can help your organization adopt new technology thoughtfully, while maintaining trust and accountability in your anti-fraud work.